BAB I
PENDAHULUAN

1.1. Latar Belakang

Sistem informasi dan dunia digital sudah menjadi bagian integral di era modern ini, dimana teknologi telah dijadikan sebagai kebutuhan utama. Namun adanya kerentanan dalam desain sistem informasi dapat membawa resiko terhadap keamanan data dan kemajuan teknologi. Keamanan *website* sangat penting dalam memudahkan pengguna untuk mencari informasi dan kebutuhan datanya, serta melindungi data pribadi pengguna. Kita hidup dizaman dimana keamanan *website* menjadi sangat penting dalam memudahkan pengguna untuk mencari berita, pengumuman, dan data yang diinginkan serta melindungi data pribadi pengguna. Namun, ada kondisi tertentu di mana sistem informasi desain kapasitas masih belum sempurna[1].

Kerentanan pada sebuah *website* dapat menimbulkan konsekuensi yang serius, seperti merusak reputasi dan kredibilitas sebuah perusahaan atau organisasi. Keamanan informasi pengguna yang tersimpan dalam *database website* yang dapat terancam oleh beberapa serangan yang berasal dari pihak yang tidak bertanggung jawab. Hal ini menjadi masalah yang signifikan. Pentingnya dalam menerapkan langkah-langkah pengamanan yang tepat dalam mencegah kebocoran dan potensi dalam kerugian besar. Perlindungan data merupakan tugas yang harus diprioritaskan dalam pekerjaan, yang memungkinkan dapat mendeteksi kerentanan keamanan sistem dan aplikasi web. Tujuannya untuk mencari metode dalam mengidentifikasi celah keamanan terhadap jaringan infrastruktur sehingga dapat mengantisipasi serangan peretas[2].

Eksistensi analisis *website* dan penilaian metodologi yang digunakan untuk mengumpulkan data sangat penting dalam proses identifikasi dalam mengurangi sebuah ancaman siber. Kerentanan uji analisis dapat dinilai dari tingkat kematangan dengan perangkat lunak sistem keamanan dari sistem keamanan itu sendiri. Ada beberapa implementasi ruang yang meliputi data, integritas data, dan aplikasi *contingency availability* pada ruang yang rusak atau error. Melakukan uji analisis

kerentanan tidak hanya melakukan dasarnya saja, melainkan proses autentikasi saat identifikasi dengan memberikan suatu ruang akses dalam melacak. Sehingga proses tersebut harus dilakukan dengan baik agar sistem yang ada berfungsi dengan baik. Administrator harus bergantung pada tiga faktor yang meliputi metode, paket, dan dependensi sehingga kemungkinan diretas melalui *server* menjadi lebih kecil[3].

Sistem informasi dan dunia digital telah mengalami perkembangan pesat di era modern ini, dimana teknologi telah menjadi sebuah hal yang tidak dapat terpisahkan dari kehidupan banyak orang sehari-harinya. Namun kemajuan teknologi juga dapat menimbulkan banyak resiko yang tergolong cukup besar terutama dalam hal keamanan *website*. Kerentanan dalam *website* dapat berdampak serius pada cakupan perusahaan ataupun organisasi, mengancam reputasi serta kepercayaan pengguna. Kebocoran data akibat serangan siber yang mengakibatkan kerugian finansial serta kepercayaan yang sulit untuk dipulihkan. Statistik dan contoh nyata dari pelanggaran data dapat memberikan pemahaman lebih dalam mengenai pentingnya keamanan *website*. Berbagai perusahaan dan organisasi telah menjadi korban serangan dunia maya, dengan data pengguna yang dicuri ataupun disalahgunakan[4]. Selain itu, serangan siber pada *website* pemerintah juga memiliki akibat yang serius. Serangan terhadap *website* pemerintah dapat mengganggu pelayanan publik, menghambat akses informasi penting, bahkan dapat merusak keamanan nasional. karena itu penting untuk memahami kerentanan dan menerapkan langkah-langkah keamanan yang tepat untuk melindungi *website* dan data pengguna[5].

Dinas AB merupakan sebuah instansi pemerintahan yang berada di Jawa Timur, yang mendedikasikan dalam mewujudkan pelayanan publik yang berkualitas dan efektif. Lembaga Instansi Pemerintahan Dinas AB memiliki peranan penting dalam memenuhi semua kebutuhan masyarakat dalam upaya pengembangan administrasi dan juga dokumen-dokumen yang dibutuhkan masyarakat. Sehingga kondisi ini dapat memberikan keterkaitan dengan pola hidup masyarakat. Hal ini memberikan contoh nyata, dimana sudah banyak masyarakat yang dimudahkan dalam mempersiapkan segala kebutuhannya, terutama yang

bersifat daring, karena hal ini dapat dijadikan sebagai bentuk upaya dari penerapan layanan masyarakat yang dilakukan oleh Dinas AB.

Berdasarkan evaluasi analisis yang dilakukan, terdapat beberapa permasalahan yang terjadi, yaitu kurangnya pemahaman mengenai faktor penyebab keamanan serangan pada sistem informasi *website* Dinas AB. Adanya kekurangan dalam penelitian terkait identifikasi dan analisis serangan keamanan yang spesifik, salah satunya kesenjangan. Hal ini terdapat dalam desain sistem ataupun kurangnya kesesuaian dalam penerapan praktik keamanan. Selain itu, terdapat kekurangan yang berfokus pada *website* Dinas AB. Keseluruhan kesenjangan yang ada pada penelitian juga mencakup berbagai jenis serangan seperti peretasan, *phising*, atau serangan *malware*. Dalam hal ini, perlu dilakukan identifikasi dan juga perbaikan terhadap kerentanan yang ada. Selain itu, belum ada upaya evaluasi menyeluruh terhadap langkah-langkah keamanan baik dalam pemantauan keamanan maupun pembaharuan prosedur yang bertujuan dalam meningkatkan kesadaran terkait praktik keamanan yang benar serta mencegah kemungkinan serangan. Selain itu, kurangnya solusi yang diteliti untuk mitigasi kerentanan di *website* Dinas AB.

Berdasarkan masalah diatas penelitian ini akan berfokus pada *website* Dinas AB, yang nantinya dapat mengevaluasi dari hasil identifikasi kerentanan spesifik, termasuk serangan seperti XSS *(Cross-site scripting)*[6]. Penelitian ini akan menggunakan berbagai *tools* pengujian keamanan seperti OWASP ZAP, Wapiti, dan Nikto untuk mendukung evaluasi keamanan sistem *website*[7]. Penelitian ini akan menunjukkan evaluasi dari jenis identifikasi kerentanan yang spesifik termasuk serangan XSS. Tidak hanya itu, diharapkan untuk dapat menemukan solusi serta rekomendasi atas temuan kerentanan yang mungkin dapat meningkatkan keamanan *website* Dinas AB, sehingga dapat memberikan kontribusi yang signifikan dalam meningkatkan kualitas pelayanan publik yang mereka berikan. Perbaikan yang dilakukan dalam proses penelitian ini dapat menghasilkan struktur yang efektif serta mendapatkan bentuk empiris yang kuat. Oleh karena itu, penulis akan melakukan evaluasi pada sistem keamanan *website* Dinas AB terhadap beberapa solusi dan temuan kerentanan yang ada menggunakan beberapa *tools* (OWASP ZAP, Wapiti, Nikto). Hal ini akan dicapai dengan memperhatikan

keamanan struktur *website* Dinas AB. Kajian tersebut memiliki implikasi secara praktis dalam meningkatkan evaluasi analisis dalam identifikasi peningkatan kualitas dan efektifitas pelayanan publik Dinas AB. Dengan melakukan analisis, akan digunakan metode evaluasi sistem kerentanan dengan mencari solusi serta rekomendasi dari kelemahan struktur *website* Dinas AB, dimana hal tersebut akan menghasilkan pemahaman yang mendalam. Temuan penelitian ini, akan memberikan manfaat nyata dalam sejumlah aspek, yaitu dengan mengidentifikasi serta memperbaiki kerentanan dan kelemahan yang ditemukan.

Kontribusi penelitian yang dapat dilakukan berdasarkan latar belakang di atas adalah tentang peningkatan sistem keamanan informasi pada *Website* Dinas AB. Penelitian ini berfokus pada evaluasi analisis kerentanan *(vulnerability assessment)* dengan menggunakan sejumlah *tools* (OWASP ZAP, Wapiti, dan Nikto). Tujuan utamanya adalah untuk mengidentifikasi dan mengatasi kerentanan keamanan yang ada di *website* Dinas AB. Dalam kajian ini, dapat dikembangkan strategi dan langkah-langkah keamanan yang lebih kuat untuk melindungi data dan informasi sensitif yang disimpan dalam sistem *database website*.

Kontribusi selanjutnya adalah metodologi analisis kerentanan pada *website* pemerintah kajian ini akan fokus pada analisis metode penyebaran kerentanan yang efektif dan efisien pada *website* pemerintah khususnya pada *website* Dinas AB. Metode yang melibatkan penggunaan *tools* analisis kerentanan, seperti analisis web, untuk mengumpulkan data dan mengidentifikasi keamanan kerentanan. Tujuan utamanya adalah untuk memberikan rekomendasi yang tepat dalam mengatasi kerentanan yang ditemukan, sehingga dapat meningkatkan keamanan dan integritas sistem *website* pemerintah tersebut. Kajian ini dapat memberikan panduan dan pedoman praktis bagi pemerintah organisasi dalam menghadapi ancaman keamanan siber dan melindungi data pengguna. Kedua kontribusi di atas diharapkan dapat memberikan kontribusi yang signifikan terhadap pemahaman dan peningkatan sistem keamanan informasi, khususnya di *website* pemerintah Dinas AB. Dengan peningkatan keamanan dan perlindungan data, reputasi dan kepercayaan publik terhadap institusi pemerintah dapat dipertahankan dan ditingkatkan.

1.2. Rumusan Masalah

Dari uraian latar belakang diatas, maka dapat dibuat rumusan masalah penelitian sebagai berikut:

1. Apakah faktor penyebab serangan keamanan pada sistem informasi *website* Dinas AB yang masih kurang dipahami?
2. Bagaimana identifikasi dan analisis munculnya serangan keamanan pada *website* Dinas AB?
3. Apa saja kerentanan yang mungkin terjadi pada *website* Dinas AB dan solusi apa yang dapat diberikan untuk mengatasinya?
4. Bagaimana Evaluasi menyeluruh terhadap langkah-langkah keamanan yang telah diterapkan pada *website* Dinas AB?
5. Apakah solusi mitigasi yang efektif untuk mengatasi kerentanan yang ditemukan di *website* Dinas AB?

1.3. Tujuan Penelitian

Tujuan penelitian ini yaitu untuk mengevaluasi keamanan *website* Dinas AB di Jawa Timur serta mengidentifikasi kerentanan yang ada. Perlu adanya upaya untuk meningkatkan pemahaman mengenai keamanan *website* Dinas AB dan dampak terhadap perlindungan data pengguna. Kemudian, menganalisis metode *vulnerability assessment* dalam *scanning* data dan analisis kerentanan pada *website* Dinas AB. Disamping itu, untuk menemukan kelemahan dan kerentanan dalam konfigurasi *website* Dinas AB serta memberikan solusi yang memadai atas temuan kerentanan, dan juga memberikan pemahaman akan ancaman keamanan yang dihadapi oleh *website* Dinas AB serta mengidentifikasi langkah-langkah perbaikan yang tepat untuk melindungi data sensitif dan peningkatan keamanan secara menyeluruh.

1.4. Batasan Masalah

Dalam pengerjaan Tugas Akhir, permasalahan yang dibahas terbatas pada beberapa hal berikut ini:

1. Penelitian ini fokus pada evaluasi keamanan *website* Dinas AB di Jawa Timur.
2. Analisis kerentanan dilakukan dengan menggunakan metode *Vulnerability Assessment* dalam *Scanning* data dan analisis kerentanan.
3. Penelitian ini membatasi ukuran sampel pada *website* Dinas AB di Jawa Timur, sehingga generalisasi hasil penelitian harus dilakukan secara hati-hati saat diterapkan pada *website* lain.
4. Evaluasi statistik digunakan untuk penelitian deskriptif, tanpa melibatkan variabel yang ada.
5. Penelitian ini memiliki batasan pada identifikasi dan analisis kerentanan yang terkait dengan desain sistem informasi *website* Dinas AB.
6. Fokus penelitian tidak mencakup serangan siber spesifik lainnya, seperti peretasan, serangan *phising* ataupun serangan *malware*.
7. Evaluasi langkah-langkah keamanan yang diterapkan pada *website* Dinas AB hanya meliputi kebijakan keamanan, pemantauan keamanan, dan juga pembaharuan prosedur yang dapat meningkatkan kesadaran akan praktik keamanan yang benar.
8. Penelitian ini memberikan solusi dan rekomendasi terhadap kerentanan yang ditemukan di *website* Dinas AB.